



US009449448B2

(12) **United States Patent**
Andersen

(10) **Patent No.:** **US 9,449,448 B2**
(45) **Date of Patent:** **Sep. 20, 2016**

(54) **CONTROLLING ACCESS TO A LOCATION**

(56) **References Cited**

(71) Applicant: **BEKEY A/S**, Høje Taastrup (DK)

U.S. PATENT DOCUMENTS

(72) Inventor: **Ebbe Andersen**, Glostrup (DK)

(73) Assignee: **Bekey A/S**, Høje Taastrup (DK)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 39 days.

5,774,058 A	6/1998	Henry et al.	
8,116,737 B2 *	2/2012	Li	H04W 8/205 455/410
2005/0044906 A1 *	3/2005	Spielman	G07C 9/00166 70/63
2010/0201536 A1 *	8/2010	Robertson	G07C 9/00904 340/686.6
2010/0306549 A1	12/2010	Ullmann	
2012/0213362 A1 *	8/2012	Bliding	G07C 9/00309 380/44

(21) Appl. No.: **14/423,092**

(Continued)

(22) PCT Filed: **Aug. 20, 2013**

FOREIGN PATENT DOCUMENTS

(86) PCT No.: **PCT/EP2013/067320**

FR	2839833 A1	11/2003
WO	WO 2006/098690 A1	9/2006

§ 371 (c)(1),

(2) Date: **Feb. 20, 2015**

(Continued)

(87) PCT Pub. No.: **WO2014/029774**

PCT Pub. Date: **Feb. 27, 2014**

Primary Examiner — Fekadeselassie Girma

Assistant Examiner — Thomas McCormack

(74) *Attorney, Agent, or Firm* — Nixon Peabody LLP

(65) **Prior Publication Data**

US 2015/0221152 A1 Aug. 6, 2015

(30) **Foreign Application Priority Data**

Aug. 21, 2012 (EP) 12181198

(51) **Int. Cl.**

G05B 19/00 (2006.01)

G07C 9/00 (2006.01)

(52) **U.S. Cl.**

CPC **G07C 9/00817** (2013.01); **G07C 9/00015** (2013.01); **G07C 9/00103** (2013.01); **G07C 9/00309** (2013.01); **G07C 2009/00825** (2013.01); **G07C 2009/00841** (2013.01); **G07C 2209/63** (2013.01)

(58) **Field of Classification Search**

None

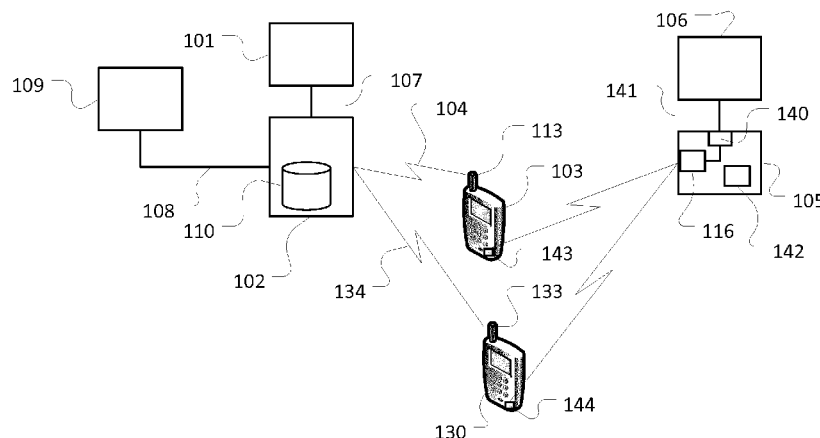
See application file for complete search history.

(57)

ABSTRACT

A method of configuring a lock control unit of an access control system. The unit has an associated lock control unit identifier and an electronic key, and can communicate via a wireless communications channel with a mobile unit and can receive an electronic key from the mobile unit to verify a received electronic key and, subject to successful verification, to activate the lock mechanism. A message having a location address is received from an access control management system. Lock control unit(s) are detected communicating via the channel in a proximity of the technician mobile unit. A respective lock control unit identifier is received from each detected unit. The unit connected to the lock mechanism is identified, based on the received identifiers. An electronic key associated with the identifier is received from the ACMS. Commands are sent to the lock control unit causing the lock control unit to perform configuration.

18 Claims, 3 Drawing Sheets



US 9,449,448 B2

Page 2

(56)

References Cited

FOREIGN PATENT DOCUMENTS

U.S. PATENT DOCUMENTS

2012/0280783 A1 11/2012 Gerhardt et al.
2012/0280790 A1* 11/2012 Gerhardt G07C 9/00309
340/5.61

WO WO 2011/034482 A1 3/2011
WO WO 2014/029774 A1 2/2014

* cited by examiner

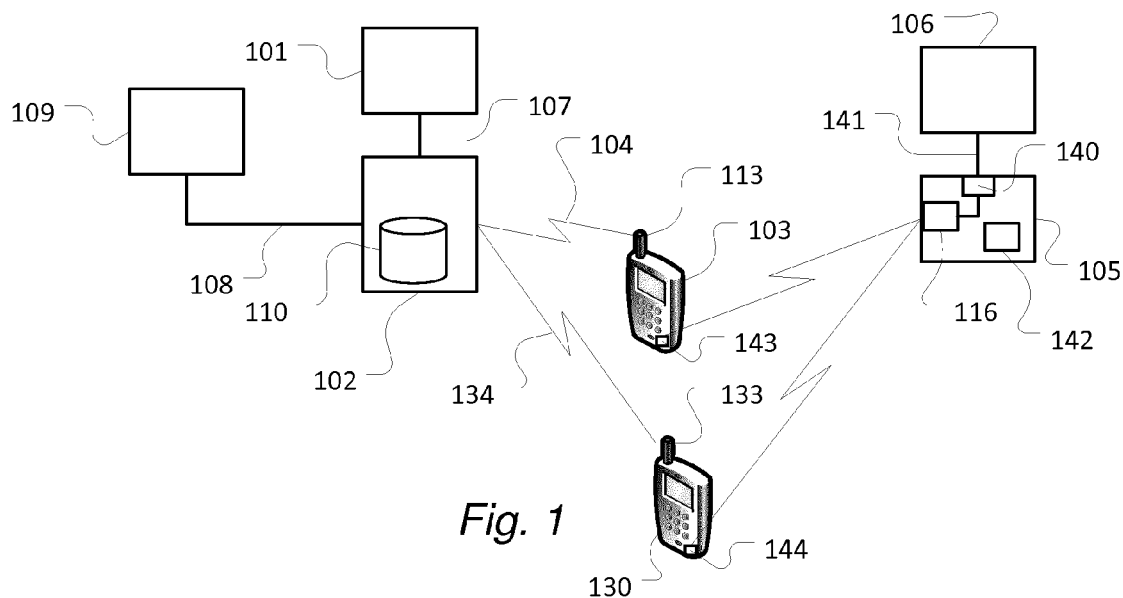


Fig. 1

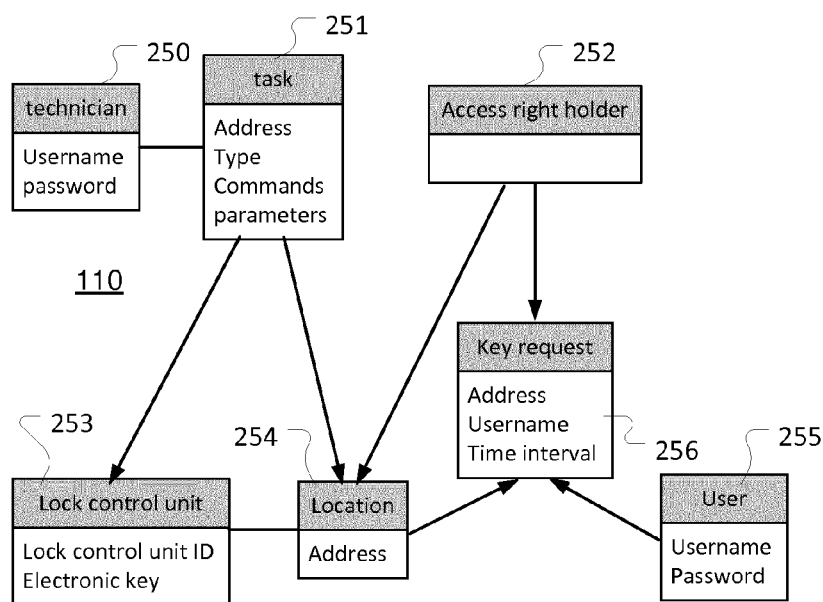


Fig. 2

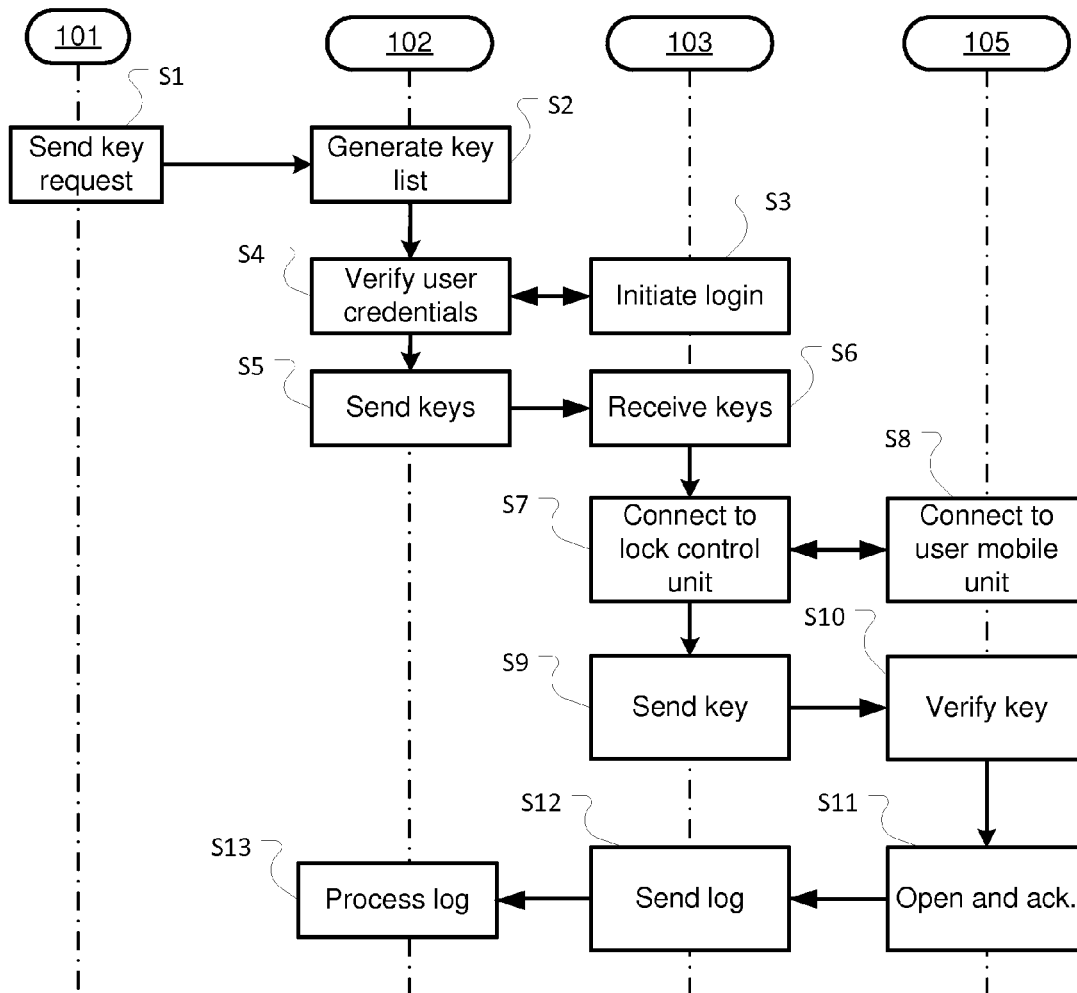


Fig. 3

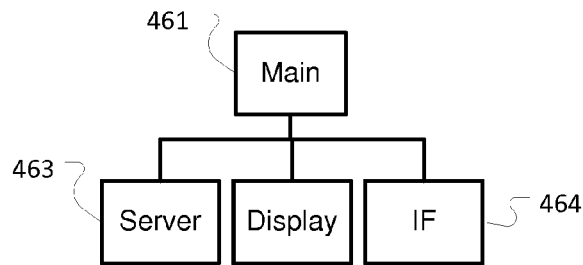


Fig. 4

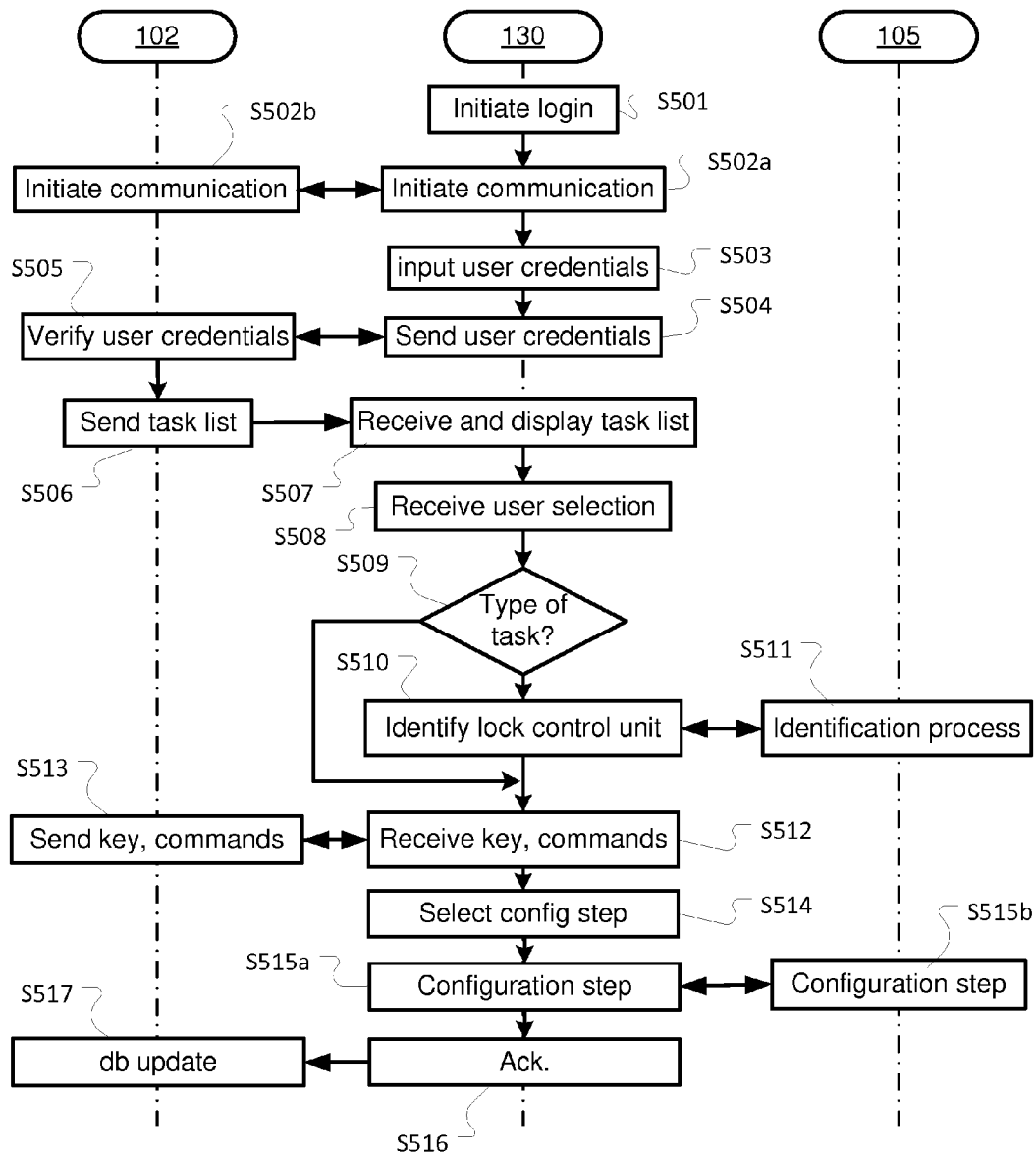


Fig. 5

1

CONTROLLING ACCESS TO A LOCATION**CROSS-REFERENCE TO RELATED APPLICATIONS**

This application is a U.S. National Stage of International Application No. PCT/EP2013/067320, filed Aug. 20, 2013, which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

The invention generally relates to controlling access to a location, where access to the location is restricted by a lock mechanism. Further the invention relates to an access control system which allows users, such as suppliers of goods or services, to access a location. More particularly, the invention relates to a method of configuring a lock control unit, e.g. during installation.

BACKGROUND

Access to many locations is restricted by access control mechanisms, in particular lock mechanisms for locking doors or other access points. Often, access to residential or commercial buildings involves unlocking a plurality of doors such as an outer or front door, an elevator door, a door to a specific part of a building e.g. to a level or floor before getting to a point of service, such as an apartment door, a mailbox, a service station or a meter for appliances, an area to be cleaned, etc.

For example in case of delivery of newspapers, the delivery person often has to gain access to a stairway in order to be able to deliver the newspapers at a locked apartment door or to put the newspaper into a mail box. Finding the correct keys in a large bundle of keys frequently causes great difficulties to the delivery person, and the locks are frequently exchanged without the delivery company being informed of this. For reasons of security it is also more and more common to lock doors or gates to backyards, residential areas or company properties, where for example refuse containers may be placed, so that the refuse collection firms have a problem quite similar to the firms that deliver newspapers. It will be appreciated that similar problems are faced by, postal delivery personal, cleaning companies, emergency physicians, domestic and other care workers, policemen, firemen, artisans, caretakers/superintendents, etc.

Some of the above service providers require access on a daily basis, while others may require access at certain time periods, such as on certain weekdays or at certain times of the day. Furthermore, different services/deliveries may require different access rights, for example firemen, security companies or police may require access to all facilities, while a mailman only requires access to a mailbox.

In order to facilitate flexible and secure management of access rights electronic access control systems exist. In particular, mobile telephones or similar mobile units have been suggested as advantageous carriers of electronic keys, since no physical keys are necessary with such systems. This means that the disadvantage of using physical keys, where keys are easily lost and difficult to find in a large bundle of keys is overcome with such a system. Furthermore, it is very easy to prohibit access to a lock control unit, when the key to this lock control unit is an electronic key, because the access request for obtaining access with an electronic is easy to deny.

2

US2002180582 discloses an efficient method and a system for controlling access to a location secured by a lock mechanism controlled by a lock control unit, which may provide a high degree of flexibility and a high level of security. This prior art method comprises storing electronic access codes in the lock control unit, and using an electronic key device for requesting access to the location by transmitting a corresponding access code from the electronic key device to the lock control unit. The lock control unit may compare the transmitted access code with the previously stored access code. The lock control unit activates the lock mechanism only if the access codes match.

EP2085934A discloses a method of controlling access to a location secured by a lock mechanism controlled by a lock control unit comprising means for wireless communication with a mobile unit. The mobile unit of this prior art performs the following steps: storing an electronic key in the mobile unit, the electronic key being indicative of a predetermined access right to the location; automatically searching for the lock control unit of the location, when the mobile unit is in a distance from the lock control unit, where wireless communication between the mobile unit and the lock control unit is established; automatically establishing a connection to the lock control unit; automatically transmitting the electronic key wirelessly to the lock control unit; and causing operation of the lock mechanism controlled by the lock control unit, whereby access to the location is obtained.

The above prior art methods and systems greatly improve the efficiency and security of managing and enforcing access rights of a large number of users and to a large number of locations. WO 2011/034482 discloses a method for updating lock access data for an electromagnetic lock. However, such systems require the manufacturing and installation of lock control units at a large number of access points. Also there may be situations where lock control units are removed from one location and newly installed at a different location. Similarly, lock control units at a location may occasionally have to be replaced by new lock control units, e.g. due to a malfunctioning of an existing lock control unit.

The manufacturing and installation of a large number of lock control units is a costly and time consuming task and also involves challenges in terms of an efficient and secure management of electronic keys. In addition to the physical deployment of lock control units and their connection to existing or newly installed lock mechanisms, a proper and efficient operation of an access control system depends on a proper functioning of the lock control unit and a proper interaction of the lock control unit with the other components of the access control system, in particular an access control management system and mobile units if the users of the system. It would thus be greatly desirable to provide a method and system for controlling access to a location that facilitates an efficient and reliable installation process of lock control units, even if many such units are to be installed and maintained.

SUMMARY

Disclosed is a method of configuring/installing a lock control unit of an access control system, the lock control unit being connected to and controlling a lock mechanism for securing a location, the lock control unit having associated with it a lock control unit identifier and electronic key verification data, the lock control unit comprising means for wireless communication via a wireless communications channel with a user mobile unit, and adapted to receive an electronic key from a user mobile unit, to verify a received

3

electronic key based on the electronic key verification data, and, subject to successful verification, to activate the lock mechanism, the method comprising performing the following steps by a technician mobile unit:

receiving a message from an access control management system, the message comprising an address indicative of the location;
 detecting one or more lock control units communicating via the wireless communications channel in a proximity of the mobile unit; and receiving from each detected lock control unit a respective lock control unit identifier;
 identifying, based on the received lock control unit identifiers, the lock control unit connected to the lock mechanism;
 sending the lock control unit identifier indicative of the lock control unit identified by the technician mobile unit to the access control management system;
 receiving, from the access control management system, an electronic key associated with the lock control unit identifier;
 sending one or more commands to the lock control unit causing the lock control unit to perform one or more configuration steps
 sending a message from the technician mobile unit to the access control management system, the message being indicative of a completion of the configuration steps;
 wherein the method further comprises associating, by the access control management system and responsive to the message indicative of a completion of the configuration steps, the lock control unit identifier of the lock control unit connected to the lock mechanism with the address of the location.

Consequently, embodiments of the method disclosed herein provide a configuration of a newly installed or existing lock control unit by means of a specifically adapted technician mobile unit, e.g. a mobile telephone executing a specifically adapted mobile application. A technician may thus use the technician mobile unit to establish communication with the lock control unit to be configured via the same wireless communications technology that is subsequently used during activation of the lock control unit by a user mobile unit. Based on an identifier identifying the lock control unit, the technician mobile unit retrieves a corresponding electronic key from an access control management system and, optionally, a number of commands identifying configuration steps to be performed during the configuration. Alternatively or additionally to configuration steps identified by commands received from the access control management system, the mobile unit may be configured to perform or initiate a number of predetermined configuration steps on the lock control unit.

In particular, embodiments of the process ensure that the technician mobile unit communicates with the correct lock control unit and that a suitable set of configuration steps are performed that match the lock control unit, thus ensuring that the installed lock control unit is responsive to the electronic key generated by or available at the access control management unit, and that the lock control unit is configured in an appropriate way ensuring correct operation of the lock control unit. Furthermore, apart from the physical installation and electrical connection, the installation process of a lock control unit typically involves one or more calibration and/or test steps. It has been realised that these steps may be performed in a reliable and consistent manner by a suitably configured technician mobile unit. Consequently, embodi-

4

ments of the method may ensure that these tests are actually performed, thus reducing the risk of malfunction of the installed lock control units.

As data is communicated via wireless data communication between the technician mobile unit and the lock control unit, a fast and convenient communication between the technician mobile unit and the lock control unit is provided without the need of physical contact. Thus, once the locksmith has activated the lock control unit at the location, the locksmith may simply use his/her technician mobile unit to configure the newly installed mobile unit, test proper operation, and report successful installation to the access control management system.

As the technician mobile unit communicates with the lock control unit using the same communication channel that is subsequently used by user mobile units when communicating with the lock control unit to gain access to the location, appropriate operation of the lock control unit and of the communication channel is verified during the configuration process.

As the technician mobile unit receives an address of the location at which a lock control unit is to be configured, the technician can to easily identify at which locations lock control units are to be installed, repaired, exchanged or otherwise performed maintenance on.

It is a further advantage of embodiments of the method described herein, that the lock control unit does not need to include any user interface, thus reducing the complexity and cost of the lock control units.

The process further comprises sending a message from the technician mobile unit to the access control management system indicative of a completion of the configuration so as to cause the access control management system to associate the lock control unit identifier of the lock control unit connected to the lock mechanism with the address of the location. Embodiments of the method described herein thus provide a mechanism for reliably and efficiently associating the installed lock control unit with a location in the computer system that manages the access control rights. In particular, the association of the identity of a newly installed lock control unit with a location in the access control management system may be performed as part of the installation process. Consequently, the system may distribute correct electronic access keys to that location without delay. This may be particularly important if the newly installed lock control unit is installed as a replacement of an existing lock control unit, as delays in the registration of the new lock control unit may otherwise result in outdated electronic keys to be distributed to users. Moreover, as the association of the lock control unit with the location in the access control system may be performed automatically without the need for a technician or other operator to manually enter lock control unit identifiers, possible sources of erroneous association are avoided.

The address indicative of the location may be a street address, a postal address, or any other suitable address format identifying the location access to which is to be controlled.

The wireless communication channel may be a short-range radio-frequency communication channel, e.g. a Bluetooth communications channel or any other suitable communications standard. Bluetooth is an industrial specification for wireless personal area networks. Bluetooth provides a way of connecting and exchanging information between devices, which comprise a Bluetooth chip or device, over a short-range radio frequency. Bluetooth devices may communicate over distances such as 5-100

5

meters. The distance may be adjusted by means of the transmission power of the Bluetooth device which sends information to another Bluetooth device which receives this information. A communications technology such as Bluetooth which allows the mobile unit and the lock control unit to automatically establish radio-communication as soon as the mobile unit is within a certain proximity of the lock control unit allow a particularly efficient access control mechanism. It is an advantage of this embodiment that the communication is based upon reliable standard components which are available as part of many devices, such as mobile phones, personal digital assistants, or the like.

The lock control unit identifier may be any suitable form of identifier for uniquely identifying a lock control unit among a plurality of lock control units. For example, the lock control unit may be a hardware identifier associated with the lock control unit or one of its components. For example, the lock control unit identifier may be an identifier associated with the communications device of the lock control unit for wireless communication with mobile units, e.g. a device address or identifier suitable for identifying the communications device in a communication system or network. For example, every Bluetooth device has a unique identity, the Bluetooth device address, which may serve as a lock control unit identifier and be used in order to identify a specific lock control unit by a mobile unit which is searching for other Bluetooth devices in the surroundings. Hence, an example of a suitable lock control unit identifier is a Bluetooth device address.

The electronic key may be any data item suitable for authenticating an access right by the lock control unit. The electronic key verification data is data stored in the lock control unit and is suitable for verification of the authenticity of an electronic key received by the lock control unit. Similarly, the access control management system may have stored therein electronic key generation data. For example, the electronic key may comprise a data item encrypted by a symmetric key shared by the lock control unit and the access control management system, and/or a data item and a message authentication code authenticating the data item based on a symmetric key shared by the lock control unit and the access control management system. The electronic key verification data and the electronic key generation data may thus each be a secret key shared by the lock control unit and the access control management system. Alternatively, the electronic key verification data and/or the electronic key generation data may be a copy of the electronic key or any other data suitable for generating and verifying an electronic key, respectively. A shared secret key may be established during manufacturing of the lock control unit and stored in the lock control unit as well as in the access control management system, e.g. associated with the lock control unit identifier.

Receiving the electronic key from the access control management system may comprise sending the lock control unit identifier from the technician mobile unit to the access control management system. The technician mobile unit or user mobile unit, as the case may be, may send a data item indicative of the received electronic key to the lock control unit so as to cause the lock control unit to verify the electronic key. The data item may be the electronic key or a suitable data item derived from the electronic key.

In some embodiments, the method may further comprise authenticating the technician mobile unit and/or a user of the technician mobile unit by the access control management system. Authentication of the technician mobile unit may be performed by any suitable mechanism, e.g. based on a

6

unique identifier of the technician mobile unit, based on a private or public key mechanism, and/or the like. Authentication of the user of the technician mobile unit may be performed by a login process requiring a user name and password or any other suitable user credentials.

Performing the one or more configuration step may comprise setting one or more configuration parameters of the lock control unit, e.g. the transmission strength of a radio transmitter of the lock control unit, thus allowing an efficient control of the configuration parameters. Alternatively or additionally, performing the one or more configuration step may comprise receiving at least one value of at least one operational parameter from the lock control unit, e.g. one or more calibration parameter.

As the configuration including the setting or calibration of operational parameters may be performed via a technician mobile unit similar to the user mobile units used during subsequent access control, the configuration may immediately be verified by the technician mobile unit without any need for further special equipment. For example, as the transmission power of the lock control unit influences the distance at which the lock control unit is detectable by a mobile unit, the technician may easily calibrate the transmission power and other parameters, e.g. a delay parameter controlling a delay between the authentication of an electronic key and the actual activation of the lock mechanism. Hence, the technician may set the operational parameters and test their suitability in an easy and efficient manner.

Some of the operational parameters may be set manually by the technician, e.g. by entering them into the technician mobile unit and causing the mobile unit to transmit a suitable command to the lock control unit for setting the corresponding parameter. Other parameters may be set based on commands and/or parameter values which the technician mobile unit has received from the access control management system, e.g. together with the electronic key. Hence, the commands communicated from the access control management system to the mobile unit may be included in, or otherwise associated with, the electronic key.

The detection of the one or more lock control units communicating via the wireless communications channel in a proximity of the technician mobile unit may be performed automatically by the technician mobile unit, e.g. by means of a wireless communication/interaction between the technician mobile unit and a lock control unit at the location. In particular, detecting one or more lock control units communicating via the wireless communications channel in a proximity of the user mobile unit may comprise detecting all electronic devices communicating via the wireless communications channel within a communication range of the technician mobile unit, and, for each detected device, determining whether the detected device is a lock control unit. The determination whether the detected device is a lock control unit may e.g. be based on one or more communications parameters, e.g. a service parameter, an automatic hand-shake or recognition protocol, a device ID or network address of the lock control unit, and/or the like. If the process identifies more than one lock control unit in a proximity of the technician mobile unit, the technician mobile unit may display a list of detected lock control units, e.g. by displaying a list of lock control unit identifiers. In one embodiment, the technician mobile unit may communicate with the access control management system so as to determine which of the detected lock control units are already associated with a location. Consequently, an embodiment of the process may present only those detected lock control units that have not yet been associated with a location;

7

alternatively the technician mobile unit may display all detected lock control units but indicate which of the displayed lock control units are not yet associated with a location.

A location may be a physical location, such as a building, an area, or some other residential, industrial, commercial or office facility, where access to the location is controlled by a lock mechanism, such as a physical lock at a door, a window, a gate or the like. Access to the location may be controlled at a single point of entry or at a plurality of access points. Furthermore, a location may also be a part of a building, area, etc., and, according to the invention, access to different parts of a location may be controlled individually, such as at an outer gate, a front door, within an elevator granting access at all or selected floors, at doors to individual apartments, offices, sections, rooms, storage facilities, such as drawers, safes, etc. The location may be stationary, such as a building, or mobile such as a vehicle, a container, a ship, or the like. Furthermore, the location may also be an installation, such as a control unit of industrial facility, an electric meter, a computer system or the like, where access to the location is controlled by a lock mechanism, such as a lock at a control box, or an electronic lock, such as a hardware lock of a computer. The term access to a location may also comprise user access to a computer or computer program where access is controlled by a software lock mechanism restricting access to a software application, to stored data, communications facilities, or the like. An access right according to the invention may be the right to interact with a location. Examples of access rights include the right to enter a building, an area, a facility, etc., the right to operate a machine, a device, a vehicle, a computer, etc., the right to open or close a door, a window, a container, a box, etc., and the right to receive or deliver goods, data information, etc., as long as the access right can be controlled by a lock mechanism.

The features of embodiments of the method described herein may be implemented in software and carried out on a mobile device or other data processing system caused by the execution of computer-executable instructions. The instructions may be program code means loaded in a memory, such as a RAM, from a storage medium or from another computer via a computer network. Alternatively, the described features may be implemented by hardwired circuitry instead of software or in combination with software.

The present invention relates to different aspects including the method described above and in the following, corresponding methods, devices, and/or product means, each yielding one or more of the benefits and advantages described in connection with the first mentioned aspect, and each having one or more embodiments corresponding to the embodiments described in connection with the first mentioned aspect and/or disclosed in the appended claims.

According to one aspect, disclosed herein is a method of controlling access to a location, the method comprising configuring a lock control unit of an access control system by performing the steps of the method described above and in the following, and performing the following steps by a user mobile unit:

receiving an electronic key from the access control management system, the electronic key being indicative of a predetermined access right to the location, the electronic key having associated with it a lock control unit identifier of a lock control unit associated with the location;

8

detecting one or more lock control units communicating via the wireless communications channel in a proximity of the user mobile unit;

identifying, based on the lock control unit identifier, the lock control unit associated with the location;

sending the electronic key to the lock control unit causing the lock control unit to authenticate the electronic key and, subject to successful authentication of the electronic key, to operate a lock mechanism.

According to another aspect, disclosed herein is a method of managing access control to a plurality of locations, each location being secured by a respective lock mechanism, each lock mechanism being controlled by a lock control unit, the lock control unit having associated with it a lock control unit identifier and electronic key verification data, the lock control unit comprising means for wireless communication via a wireless communications channel with a user mobile unit, and adapted to receive a data item indicative of an electronic key from a user mobile unit, to verify a received electronic key based on the electronic key verification data and, subject to successful verification, to activate the lock mechanism, the method comprising performing the following steps by an access control management system:

sending a message to a technician mobile unit, the technician mobile unit comprising means for wireless communication via the wireless communications channel with the lock control unit, the message comprising an address indicative of the location;

receiving from the technician mobile unit, a lock control unit identifier indicative of a lock control unit identified by the technician mobile unit to be connected to a lock mechanism of the location;

sending to the technician mobile unit an electronic key associated with the lock control unit identifier, causing the technician mobile unit to send one or more commands to the lock control unit causing the lock control unit to perform one or more configuration steps;

receiving a message from the technician mobile unit, the message being indicative of a completion of the configuration steps; and

associating, responsive to the received message, the lock control unit identifier of the lock control unit connected to the lock mechanism with the address of the location.

According to a further aspect, disclosed herein is an access control management system configured to perform the steps of the method of managing access control to a plurality of locations described herein.

The access control management system may be a suitably programmed data processing system. The access control management system may comprise a database having stored therein data records indicative of a plurality of respective locations and data records of a plurality of lock control units. Each data record indicative of a lock control unit may comprise or be associated with a lock control unit identifier and corresponding electronic key generation data. Each data record indicative of a location may comprise or be associated with an address. During an embodiment of the configuration process disclosed herein, the access control management system may be adapted to establish an association between a data record indicative of a location and a data record indicative of a lock control unit.

According to yet a further aspect, disclosed herein is a technician mobile unit configured to perform the step of the method of configuring a lock control unit described herein. Each of the user and technician mobile units may be specifically designed, portable units for use in the access control system described herein. Alternatively, a user or

technician mobile unit may be a mobile communications device, such as a mobile telephone, smart phone, or the like, for voice and/or data communication via a cellular telecommunications network. Many such devices comprise short range, wireless communications interfaces allowing communication with a lock control unit, and they can be programmed by suitable software to perform the steps of embodiments of the process described herein.

According to yet another aspect, disclosed herein are embodiments of a lock control unit. The lock control unit is connectable to and adapted to control a lock mechanism for securing a location, the lock control unit having associated with it a lock control unit identifier and electronic key verification data. The lock control unit comprises a processing unit and first wireless communications means adapted to communicate with wireless communication means of a technician mobile unit, the lock control unit being configured to receive an electronic key and one or more commands from a technician mobile unit, to verify the received electronic key based on the electronic key verification data and, subject to successful verification, to perform one or more configuration steps responsive to the received one or more commands.

According to another aspect a computer program comprises program code means for causing a data processing system or device to perform the steps of one or more of the methods disclosed herein, when said computer program is executed on the data processing device or system.

According to yet another aspect, disclosed herein are embodiments of a lock control unit operationally connectable to a lock mechanism and adapted to control the lock mechanism for securing a location, the lock control unit having associated with it a lock control unit identifier and electronic key verification data, and comprising a processing unit, and first wireless communications means adapted to communicate with wireless communication means of a user mobile unit, the lock control unit being configured to receive a data indicative of an electronic key and one or more commands from a user mobile unit, to verify the received electronic key based on the electronic key verification data and, subject to successful verification, to activate the lock mechanism, and to send a message to the user mobile unit indicative of one or more operation parameters of the lock control unit.

Hence, an efficient mechanism is provided for communicating operational information of the lock control units to the access control management system via the user mobile unit, thus allowing the access control management system to monitor operation of the lock control units and/or detect lock control units that are not operating properly or that otherwise require maintenance. Such maintenance may then even be initiated using embodiments of the method for configuring a lock control unit as described herein. It is a further advantage that the lock control unit does not need any other communications means or interface for communicating with the access control management system or another entity to detect lock control.

Accordingly, disclosed herein is a user mobile unit adapted to receive an electronic key from an access control management system, the electronic key being indicative of a predetermined access right to a location, the electronic key having associated with it a lock control unit identifier of a lock control unit associated with the location; to detect one or more lock control units communicating via the wireless communications channel in a proximity of the user mobile unit; to identify, based on the lock control unit identifier, the lock control unit associated with the location; to send a data

item indicative of the electronic key to the lock control unit causing the lock control unit to authenticate the electronic key and, subject to successful authentication of the electronic key, to operate a lock mechanism; to receive a message from the lock control unit indicative of at least one operational parameter of the lock control unit; and to send a message indicative of the received operational parameter to the access control management system.

In particular, in some situations, it may be difficult or even impossible to connect the lock control unit with an external power source. In such situations it may be desirable to provide the lock control unit with its own battery. It would thus be unfortunate when the lock control unit fails to function properly due to an unexpected low battery level. Accordingly, in some embodiments the lock control unit comprises a battery for providing power to the lock control unit, and the operational parameter comprises a battery status of the battery.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and/or additional objects, features and advantages of the present invention, will be further elucidated by the following illustrative and nonlimiting detailed description of embodiments of the present invention, with reference to the appended drawings, wherein:

FIG. 1 schematically illustrates an access control system.

FIG. 2 illustrates an example of a database structure of a database of an access control management system.

FIG. 3 shows a flow diagram illustrating the access control process.

FIG. 4 shows a functional block diagram of the functional blocks of a program stored on and executed by the technician mobile unit.

FIG. 5 shows a flow diagram illustrating an embodiment of a configuration process performed by the technician mobile unit.

DETAILED DESCRIPTION

In the following description, reference is made to the accompanying figures, which show by way of illustration how the invention may be practiced.

FIG. 1 schematically illustrates an access control system.

The system comprises an access control management system 102, an access right management system 101, a user mobile unit 103, a lock control unit 105, a lock mechanism 106, and a technician mobile unit 130. For ease of illustration, FIG. 1 only shows a single user mobile unit, a single technician mobile, a single lock control unit, and a single lock mechanism. It will be appreciated, however, that embodiments of an access management system typically comprise a plurality of each of these units, as the access control system typically manages access to a plurality of locations, each location having one or more lock control units associated to it, and manages access rights of a plurality of users, each user having an associated user mobile unit. Likewise, embodiments of the system may include a plurality of technician mobile units, thus allowing a plurality of technicians to concurrently support the lock control units of the system. An embodiment of the access control system may further comprise more than one access right management systems, e.g. a system of a newspaper delivery company, another system of a domestic care company, and/or the like.

Each of the access control management system 102 and the access rights management system 101 may be implemented as a separate, suitably programmed data processing

11

system. The respective systems may communicate with each other via any suitable communications interface **107**, e.g. a computer network or other communications network. Alternatively, the access control management system and the access rights management system may be implemented as separate software systems executed on the same data processing system and communicating with each other via any suitable data communications mechanism, such as a suitable API, a common database, and/or the like.

The access right management system **101** may be a data processing system managing the access rights of a plurality of users to a plurality of locations. For example, the access right management system may be a data processing system of a service company, e.g. a cleaning company, a home care company, a security company, a delivery company, etc., managing access rights of its service personnel to the locations at which the service company performs its service.

For example, a newspaper company has a number of subscribers who are to have their newspaper delivered to their respective residence. Information on the subscribers may be kept in a database of (or accessible to) an access right management system of the newspaper company. The information on subscribers may comprise their residence address, when they should receive a newspaper etc. In this example, the access right management system may send a request to the access control management system including information about the delivery persons who are to be granted access to certain locations, and optionally additional attributes, such as timing information regarding the access right, etc. In one embodiment, the access rights management system may send the information in the form of data records, each record including a user identifier identifying a user to be granted access, a location identifier identifying the location to which the user is to be granted access to, and a validity period indicative of the time or time interval during which access is to be granted. For example, the user identifier may be a username or any other suitable identifier. The location identifier may be a street address or any other suitable identifier.

The access control management system **102** may comprise an access control database **110** having stored therein user records identifying registered users. Each user record may be identified by a user identifier or other suitable key and additional information regarding the user such as an identifier identifying a mobile unit associated with the user, user credentials allowing authentication of the user when the user requests access keys, and/or additional or alternative information. The access control database may further comprise location records identifying locations. Each location may include an address identifying a street address of the location and each location record may identify a lock control unit associated to that location.

The database may further comprise lock control unit records associated with respective lock control units. Each lock control unit record may comprise information about a communications address, an access key, and optionally further attributes. The communications address may e.g. comprise a Bluetooth device address or other suitable address identifying the lock control unit in a suitable communications technology allowing a mobile unit to identify and communicate with the lock control unit using said communications technology. It will be appreciated that such a database may be organised in a variety of ways so as to associate lock control units with respective locations, to associate mobile units with respective locations, and optionally to associate users with respective mobile units. Hence, based on the information received from the access rights

12

management system, the access control management system may identify which mobile units are to receive which electronic keys.

The access control management system **102** may further comprise an interface **108** to a lock control unit manufacturer system **109**, e.g. a data processing system of a manufacturer of lock control units. The access control system may receive data associated with newly manufactured lock control units directly from the lock control unit manufacturer system. These data may include a lock control unit identifier and electronic key generation data associated with each lock control unit.

The user mobile unit **103** may be a mobile phone, a PDA (personal digital assistant), a handheld computer, another terminal that is adapted to emit a Bluetooth or other radio-based signal or other type of signal which can be received by a lock control unit controlling access to the location, and to communicate with the access control management system. A mobile unit may also be mountable on or in a vehicle.

The user mobile unit **103** is equipped with a communications interface **143** for transmitting signals via a wireless communications channel to the lock control unit **105**. The communication may utilise Bluetooth or other radio communication, or any other suitable communications technology. The communication may follow a proprietary protocol or, preferably, a standard protocol such as Bluetooth, TCP/IP, IrDa, a telephone data protocol, a mobile telephone data protocol, http, sound, etc. The information may be transferred either using a proprietary data format or, preferably, a standard format, such as wml, html, binary code, machine code, AT-commands, voice commands or the like.

The mobile unit **103** is equipped with a communications interface, for example the transmit/receive aerial (antenna) **113** and associated radio communications circuitry of a mobile phone, allowing the mobile unit **103** to establish data communication with the access control management system **102**. The communication may be a radio-based communication, preferably via a standard communications network for example a standard mobile telephone network. Via the communications link **104** between the mobile unit **103** and the access control management system **102**, electronic keys may be transmitted from the access control management system **102** to the mobile unit **103**. Furthermore, log data may be transmitted from the mobile unit **103** to the access control management system **102** via the communications link **104**. This data transmission may utilise the so-called Short Message Service (SMS) or other higher speed data channels, e.g. GSM data, WAP or various data channels of CDMA transmission systems. Alternatively or additionally, other suitable communications channels using a proprietary or standard protocol such as TCP/IP, http, voice messages, etc. may be used.

A user mobile unit **103** can be used by a user, e.g. a newspaper delivery man, to gain access to a location, e.g. a locked stairway in a building, where subscribers have their residence. Before the mobile unit **103** can be used in the access control system, the mobile unit may need to be registered with the access control management system **102**. For example, in embodiments, where the mobile unit is implemented as a mobile telephone, the telephone number of the mobile unit **103** may be set up in the access control management system **102**. The telephone number may be related to a SIM card which is inserted in the mobile unit **103**. The mobile unit may have stored thereon an application such as a Java program, a mobile application, or the like, programmed to communicate with the access control management system to receive access keys, and to communicate

13

with the lock control units to send a corresponding access key. The application may be installed on the mobile unit during an initial setup and registration process.

When data items comprising electronic keys are received by the user mobile unit **103** from the access control management system **102**, they may be stored in a memory of the mobile unit or on a memory associated with the mobile unit, e.g. the SIM card. The user mobile unit **103** may be adapted to automatically initiate the transmission of the electronic key via the wireless communications channel to a corresponding communications interface **116** of the lock control unit **105**. The wireless communications technology, such as Bluetooth, used for communicating electronic keys between the user mobile unit **103** and the lock control unit **105** may allow for an automatic mechanism for initiating communication and exchanging data when the mobile unit enters a communications range of the lock control unit. This allows for a fast transmission of the electronic key to the lock control unit **105** and, therefore, a short response time from when the mobile unit **103** approaches the lock control unit until an activation of the lock mechanism **106** to grant the user of the user mobile access to the location. Furthermore, the Bluetooth transmission has the advantage that it does not involve costs for using a communications network.

The technician mobile unit **130** may be a mobile phone, a PDA (personal digital assistant), a handheld computer, another terminal that is adapted to emit a Bluetooth or other radio-based signal or other type of signal which can be received by a lock control unit, and to communicate with the access control management system.

The technician mobile unit **130** is equipped with a communications interface **144** for transmitting signals to the lock control unit **105** using the same wireless communications channel as the communication between the user mobile unit and the lock control unit. The technician mobile unit **130** is further equipped with a communications interface, for example the transmit/receive aerial (antenna) **133** and associated radio communications circuitry of a mobile phone or other wireless communications device, allowing the technician mobile unit **130** to establish data communication with the access control management system **102**. The communication may be a radio-based communication, preferably via a standard communications network for example a standard mobile telephone network. Via the communications link **134** between the technician mobile unit **130** and the access control management system **102**, task lists, electronic keys and commands may be transmitted from the access control management system **102** to the technician mobile unit **130**. Furthermore, log data may be transmitted from the technician mobile unit **130** to the access control management system **102** via the communications link **134**. This data transmission may utilise the so-called Short Message Service (SMS) or other higher speed data channels, e.g. GSM data, WAP or various data channels of CDMA transmission systems. Alternatively or additionally, other suitable communications channels using a proprietary or standard protocol such as TCP/IP, http, voice messages, etc. may be used. The communications channel **134** used for communicating between the technician mobile unit **130** and the access control management system **102** may be the same or a different communications channel as is used for communication between a user mobile unit **13** and the access control management system **102**. For example, the technician and user mobile units may use different mobile telecommunications networks.

A technician mobile unit **130** can be used by a technician, such as a locksmith, to configure and/or test a newly

14

installed or existing lock control unit **105**. Before the technician mobile unit **130** can be used in the access control system, it may need to be registered with the access control management system **102**, e.g. in a similar manner as a user mobile unit. The communication and operation of a technician mobile unit may be similar as a user mobile unit. However, the technician mobile unit is configured to perform configuration tasks, as will be described in greater detail below. To this end, the technician mobile unit may have stored thereon an application such as a Java program, a mobile application, or the like, programmed to communicate with the access control management system and with the lock control units. The application may be installed on the mobile unit during an initial setup and registration process.

The lock control unit **105** comprises a communications interface **116**, e.g. a Bluetooth device, for communicating with user mobile units **103** and technician mobile units **130**. The lock control unit **105** is further connected to the lock mechanism **106**.

The lock control unit further comprises a processing unit **140** which is adapted to verify received electronic keys. If the received electronic key is valid, the processing unit may send a control signal to the lock mechanism **106** for operating the lock mechanism and thereby granting access to the location. The lock control unit may further comprise a battery **142** or other suitable energy source. Alternatively or additionally, the lock control unit may receive electrical power from an external energy source.

The lock mechanism **106** may be a door lock system, a valve control system, or the like. The connection **141** between the lock control unit and the lock mechanism may be an electrical or mechanical connection or a wireless communications link. Alternatively, instead of a separate lock mechanism **106**, the lock control unit **105** itself may contain corresponding electrical, electronic and/or mechanical components, such as an electric engine which could open a valve, or an electric device which could open a door. The lock mechanism **106** comprises a unit which, for example via an electrical/electronic relay, can activate a lock (not shown) which is for example mounted on a door. The lock mechanism **106** may be connected to an existing door telephone system in a building, or it may be adapted to operate independently, via its own mechanical parts and its own power supply.

The lock control unit may thus be added to an existing electrical system, which is otherwise used to perform unlocking of the door, e.g. from a telephone in a flat which is connected to the entry telephone. The lock control unit may thus work in parallel with an entry telephone or another suitable lock control system. Since entry telephones or similar lock systems are already installed at many doors which give access to flats, it may be easy, fast and non-expensive to provide a control module to these existing lock systems, where the control module may comprise a Bluetooth receiver, an electrical power input and an output for controlling the opening of the lock.

FIG. 2 illustrates an example of a database structure of a database **110** of an access control management system, e.g. access control management system **102** of FIG. 1. The database may be implemented as a relational database comprising a plurality of tables. It will be appreciated, however, that the database may be implemented as any other suitable database structure.

15

The database comprises a table **254** of location records, each location record identifying a location. Each location record may e.g. comprise a field indicative of the address of the location.

The database further comprises a table **253** of lock control unit records, each identifying a lock control unit. Each lock control unit record may comprise respective fields indicative of the lock control unit ID and electronic key generation data for one or more electronic keys associated with the lock control unit. The electronic key generation data may e.g. comprise the electronic key itself or a secret key suitable for generation of an electronic key e.g. by encrypting a data item, by generating a message authentication code, or the like. The lock control unit ID may be a serial number of the lock control unit. Alternatively the lock control unit may be an identifier that identifies the communications device of the lock control unit in the communications protocol used by the lock control unit. For example, in embodiments where the lock control unit communicates with user mobile units and technician mobile units via a Bluetooth communications channel, the lock control unit ID may be the Bluetooth device address of the Bluetooth transceiver of the lock control unit. The access control management system may receive the lock control unit records from the manufacturer of the lock control units.

The database further comprises a table **252** of access right holder records, each indicative of an access right holder. Each access right holder may be associated with one or more locations, and each location may have one or more access right holders associated with it. An access right holder may be the owner of the location or another party to which access right has been granted, e.g. a service company, a newspaper company, a delivery company, etc.

The database further comprises a table **255** of user records, each identifying a user who may be authorised by the access right holder to access a location. Each user record may include fields identifying the user's user name and password or other user credentials.

The database further comprises a table **256** of key request records, each key request record associating a user with a location. To this end the access control management system may receive data records from an access right holder, identifying a user (e.g. by means of a user name), a location (e.g. by means of an address), and optionally a validity period indicating a time interval during which the user should be granted access to the location.

The database further comprises a table **250** of technician records, each identifying a technician who may be assigned installation/configuration tasks for installing or otherwise configuring lock control units at locations. Each technician record may include fields identifying the technician's user name and password or other user credentials.

The database further comprises a table **251** of task records, each identifying a technician task to be performed by a technician and at a given location. A task may involve installation of new lock control unit, replacement of an existing by a new lock control unit, maintenance of an existing lock control unit, and/or the like. To this end the task record may include identifying a task type. A task record may further include fields identifying the address at which the task is to be performed, and commands and/or parameters for use during the task. An example of a process for assigning a task to a technician and for completing a task using a technician mobile unit will be described in more detail below.

As part of the configuration process, the access control management system receives information about which lock

16

control unit is installed at the location at which the configuration task has been performed. This allows the database to associate a lock control unit from table **253** with a location from table **254**. Consequently, when the system subsequently receives a key request for a given location, the access control management system may use the database to identify which lock control unit is installed at that location and, thus, which electronic key to send to the user identified by the key request.

It will be appreciated that the above information may be organised in tables in a different manner, and that tables may include additional or alternative information.

FIG. 3 shows a flow diagram illustrating the access control process, e.g. as performed by the access control system shown in FIG. 1.

In step **S1**, the access rights management system **101** communicates one or more data records to the access control management system **102**, each data record indicative of a key request. Each key request may include an identifier identifying the user to which the access right is to be granted, and identifier identifying the location to which access is to be granted, and a time interval indicative of the time period during which access should be granted.

In step **S2**, the access control management system generates respective lists of electronic keys for respective users. Based on the key requests from the access right management system, the access control management system may for each user maintain a list of electronic keys to be communicated to the user. For example, the list may comprise the electronic keys associated with all key requests for that particular user that have a validity time interval which expires within a predetermined time window, e.g. the next 24 hours, the next week, or another suitable time window. Alternatively, the access control management system may generate the list responsive to a request from a user.

Each time a user mobile unit **103** should be used as an electronic key device for obtaining access to a number of locations, a number of steps may be performed in order to install the electronic keys in the mobile unit **103** for the respective lock control units. The user mobile unit may initiate a communications session with the access control management system (step **S3**) so as to download electronic keys. This may be done upon start-up of the mobile unit or upon start-up of a corresponding software application executed by the mobile unit, or triggered by a user input. The communication may be established using any suitable communications protocol providing suitably secure communication, e.g. using a TCP/IP connection via the internet and employing Transport Layer Security (TLS). The user is requested to authenticate himself/herself, e.g. by providing a username and password, or other suitable credentials, which are verified by the access control management system (step **S4**). Alternatively or additionally, the login may be subject to other authentication procedures, e.g. an authentication of the user mobile unit. In some embodiments, the user mobile unit may further send a unique hardware ID to the access control management system, e.g. a Bluetooth device address of the Bluetooth device of the user mobile unit.

Subject to successful authentication in step **S4**, in step **S5** the access control management system transmits the generated list of electronic keys to the user mobile unit. The electronic keys may be communicated to and stored (step **S6**) by the user mobile unit in encrypted form, e.g. by an encryption key derived from the user name, password, and

17

hardware ID of the mobile unit. If there are no keys for the user mobile unit, the user mobile unit may terminate the software application.

When the user subsequently approaches a lock control unit, the user mobile unit **103** detects lock control units in its vicinity (step S7). For example, the user mobile unit may operate as a Bluetooth client and scan for other Bluetooth devices in its vicinity. The mobile unit may then determine whether the detected Bluetooth devices are lock control units of the access control system. This determination may e.g. be based on the Bluetooth profile of the lock control unit, or on any suitable hand-shake process. To this end, the lock control unit **105** may act as a Bluetooth server and provide a predetermined profile (step S8). As a part of the determination, the user mobile unit receives a lock control unit ID from the lock control unit. For example, the Bluetooth device address of the lock control unit may serve as a lock control unit ID. The user mobile unit determines whether it has stored an electronic key associated with the lock control unit ID of the detected lock control unit. If this is not the case, the process may continue to scan for lock control units in the vicinity of the user mobile unit. Otherwise the user mobile unit establishes a wireless connection with the lock control unit, e.g. a Bluetooth connection. The wireless connection may be secured to obtain authenticity and privacy using any suitable protection mechanism, e.g. based on private or public keys. For example, when the communication is based on a private key, the lock control unit may be provided with its private key during manufacturing; and the access control management system may receive the private key together with the lock control ID of the lock control unit, e.g. the lock control unit's Bluetooth address. The mobile unit may thus receive the private key as a part of the data package including the electronic keys.

In step S9, the user mobile unit forwards an electronic key to the lock control unit, optionally together with a command and a time interval. For example, the user mobile unit may receive the electronic key comprised in an encrypted data package, where the data package includes the electronic key and its validity period. The data package may be encrypted using a symmetric key known only to the lock control unit and the access control management system. This symmetric key may e.g. be established during manufacturing of the lock control unit and registration of the lock control unit with the access control management system. Hence, the electronic key generation data stored by the access control management system and the electronic key verification data stored by the lock control unit comprises the symmetric key.

In step S10, the lock control unit verifies the received electronic key based on the electronic key verification data stored by the lock control unit. For example, the lock control unit may decrypt the received message using the electronic key verification data, and compare the decrypted message with a verification code included associated with the message. The lock control unit may further verify a validity period of the electronic key. To this end, the lock control unit may further receive a time stamp indicative of the current time from the user mobile unit. Alternatively, the lock control unit may comprise a timer or clock allowing the lock control unit to determine the current time.

In step S11 and subject to successful verification, the lock control unit activates the lock mechanism and returns and acknowledgment message to the user mobile unit. In some embodiments, the lock control unit may include one or more operational parameters in the acknowledgement message or communicate such operational parameters to the user mobile unit in a separate message.

18

In step S12, the user mobile unit forwards a log message to the access control management system including information about the successful access to the location. The user mobile unit may then return to step S7 to continue scanning for lock control units. It will be appreciated that, in some embodiments, log messages may not be sent individually after each lock activation, but collected by the mobile unit and forwarded to the access control management system at a later point in time.

The log message may be stored and/or otherwise processed by the access control management system (step S13). In some embodiments, the user mobile unit forwards one or more operation parameters received from the lock control unit to the access control management system, thus allowing the access control management system to monitor correct operation of the lock control unit. If necessary, the access control management unit may thus initiate maintenance on the lock control unit.

For example, some lock control units may be battery driven, and the operational parameter may be a battery status, a low battery flag, or the like, thus allowing the access control management system to create an alert or otherwise initiate a maintenance task where a technician or other person exchanges the battery of the lock control unit.

FIG. 4 shows a functional block diagram of the functional blocks of a program stored on and executed by the technician mobile unit. It will be appreciated that a user mobile unit may have software installed similar to the software of the technician mobile unit, where some modules even may be the same, thus allowing reuse of major parts of the program code, and ensuring that the tests and calibrations performed by a technician mobile unit provide reliable information about the subsequent operation of the system when a user mobile unit is used to communicate with the lock control unit.

The program comprises a main module **461**, a display module **462**, a server module **463**, and an interface module **464**.

The display module **462** controls the display of information on the display of the mobile unit and the receipt of user-input. The server module **463** handles the communication between the mobile unit and the access control management system using the available communications services, such as webservices, of the mobile unit. In particular, the server module provides functionality for exchanging login information, receiving tasks lists, receiving electronic keys and commands, sending acknowledgement and log messages, and/or the like. Optionally, the server module may provide additional functionality, e.g. functionality for receiving time information from the access control management system and for setting the internal clock of the mobile unit based on the received time information, thus ensuring that clock of the mobile unit is not tempered with and that time information (e.g. time stamps of messages) communicated from the mobile unit is accurate. Other examples of functionality provided by the server module include receiving and executing commands from the access control management system, e.g. commands causing the server module to download and install software updates, to perform a forced logout, etc.

The interface module **464** provides functionality for the communication between the mobile unit and the lock control unit using a suitable communication technology, such as Bluetooth. In particular, the interface module provides functionality for detecting lock control units in the vicinity of the

mobile unit, for sending electronic keys and commands to the lock control unit, and for receiving messages from the lock control unit.

FIG. 5 is a flow diagram illustrating an embodiment of a configuration process performed by the technician mobile unit 130, e.g. under the control of a program as described with reference to FIG. 4 above.

Prior to installing a given lock control unit at a location, the location and the lock control unit are typically registered in the access control management system 102. Information about locations, e.g. street addresses, may be entered by an operator or received from an external database of addresses, or in any other suitable manner. During production of lock control units, they may be equipped with a communications interface device, e.g. a Bluetooth interface, having an associated interface device ID (e.g. a Bluetooth device address), and programmed with electronic key verification data for one or more electronic keys. Data indicative of lock control units may be entered into the access control management system by an operator or be received from an external system, e.g. a system of a manufacturer of lock control units. The access control management system may e.g. receive a data record for each lock control unit to be used in the access control system. Each data record may e.g. comprise a lock control unit ID, e.g. a serial number, an interface device ID, and electronic key generation data for the one or more electronic keys.

When the technician application is started on the technician mobile unit 130, the main module initialises (step S501) the program and controls the subsequent process.

Subsequently, the server module contacts the access control management system and a communications link is established between the technician mobile unit (step S502a) and the access control management system (step S502b). The communication may be established using any suitable communications protocol providing suitably secure communication, e.g. using a TCP/IP connection via the internet and employing Transport Layer Security (TLS).

In step S503, the display module causes a login dialog to be displayed on the display of the technician mobile unit, and a user is requested to authenticate himself/herself, e.g. by providing a username and password, or other suitable credentials. The display module receives the login information entered by the user and forwards the received information to the main module. Alternatively or additionally, the login may be subject to other authentication procedures, e.g. an authentication of the technician mobile unit. In some embodiments, the technician mobile unit may further send a unique hardware ID to the access control management system, e.g. a Bluetooth device address of the Bluetooth device of the technician mobile unit.

In step S504, the login information is forwarded via the server module to the access control management system 102 for validation, and the access control management system verifies (step S505) the user credentials so as to authenticate the user as an authorized technician, based on user data stored in its database.

In step S506 and upon successful user validation, the access control management system sends a list of maintenance tasks to the technician mobile unit. For example, the task list may be generated based on requests received by the access control management system from access right holders to add one or more locations to the access control system, thus requiring installation of a lock control unit at those locations. The task list may further be based on error reports or maintenance requests received for existing lock control units.

In step S507, the server module of the technician mobile unit receives the task list. If the task list is empty, the user may log off the system; otherwise the process displays the task list on the display of the mobile unit. The task list may comprise a list of locations (e.g. identified by street addresses) at which lock control units are to be installed. It will be appreciated that the task list may comprise additional information, such as a type of task to perform (e.g. installation of a new lock control unit, maintenance of an existing lock control unit, replacement of an existing lock control unit with a new lock control unit, and/or the like), or other relevant information.

In step S508, the technician mobile unit receives a user-selection of one of the listed tasks. Upon selection of a task, additional task-related information may be displayed. When the user confirms the selection of one of the tasks, the process proceeds to step S509; otherwise the process awaits a different selection. It will be appreciated that the selection of a location may be performed in a different manner. For example, the mobile unit may receive information about a single task only, without allowing the technician to select from a list. In another embodiment, some or all tasks may be associated with multiple addresses, and the process may first let the technician select a task, then receive the locations associated with the selected task, and let the technician select one of the received locations.

As mentioned above, there are different types of tasks that may be performed by a technician including e.g. installation of a new lock control unit, replacement of an existing by a new lock control unit, maintenance/repair of an existing lock control unit. The further process flow may depend on the type of task to be performed. Accordingly, in step S509, the mobile unit determines a type of task, e.g. based on an attribute associated with the location and received from the access control management system. If the type of task indicates that a new lock control unit is to be installed at the address, the process proceeds at step S510; if the type of task indicates that the technician is to perform maintenance of an existing lock control unit, the process proceeds at step S512. It will be appreciated, that alternative embodiments may include more or fewer task types, and the process may be divided in more or fewer alternative branches.

In step S510, the main module controls the display module to display a user-interface allowing the user to initiate a scan of lock control units. When the technician has performed the physical installation of a lock control unit, the technician may thus start the scan process. When the display module receives a user input indicative of a command to initiate a scan, the main module controls the interface module to identify all lock control units from which a communications signal is received. During the identification process the lock control units 105 send their lock control unit IDs, e.g. their Bluetooth device addresses, to the technician mobile unit (step S511).

The main module further controls the display module to display a list of lock control unit IDs of the lock control units detected during the scan, thus allowing the technician to select the newly installed lock control unit from the list. To this end, the lock control unit may have its control unit ID or another suitable identifier printed on it or may be marked in another suitable manner allowing the technician to identify the lock control unit ID. For example, the lock control unit may comprise a label, a bar code, or another machine and/or human readable insignia or device. Upon receipt of a user selection of a lock control unit, the process proceeds at step S512.

21

In step S512, the main module controls the server module to request from the access control management system an electronic key including configuration commands associated with the selected lock control unit. The commands indicate a set of configuration commands to be sent to the lock control unit during the configuration setup. In step S513, the access control management system sends the electronic key and the commands to the technician mobile unit. Upon receipt of the electronic key and commands from the access control management system, the main module determines one or more configuration steps consistent with the received commands and controls the display module to display a list of available configuration steps.

In subsequent step S514, the process awaits a user input indicative of a selection of one of the configuration steps from the list, or an input indicative of a completion of the configuration process. If the received input is indicative of a configuration step, the process proceeds at steps S515a and S515b; otherwise, if the received user selection of a completion of the configuration process, the process proceeds at step S516 to complete the configuration process. In some embodiments, one or more of the configuration steps may be mandatory to be performed before the configuration process may be completed. In such embodiments, the display module may prevent the selection of the completion option until all mandatory configuration steps have been performed. An example of a mandatory configuration step may be a step where the mobile unit sends an "open door" command to the lock control unit, thus allowing the technician to verify that the lock control unit successfully activates the lock mechanism.

In step S515a, the technician mobile unit communicates with the lock control unit to cause the lock control unit to perform the selected configuration step (step S515b), e.g. causing the setting of a configuration parameter in the lock control unit, the sending of an operational parameter value from the lock control unit to the technician mobile unit, and/or the like. Examples of configuration steps will be described in more detail below. A configuration step typically comprises the main module causing the interface module to send a message to the lock control unit, the message including the electronic key, a command, and optionally one or more parameters. The parameter may e.g. be a parameter received from the access control management system or a parameter input by the technician. To this end, upon selection of a configuration step, the display module may prompt the user to input an associated parameter value. The message causes the lock control unit to verify the received electronic key, to perform the received commands, and to return an acknowledgment message to the mobile unit indicative of a result of the command. The result may be displayed on the mobile unit by the display module. Examples of result may include failure to verify the electronic key, failure or acknowledgement of successful performance of the command, one or more parameter values indicative of an operation parameter of the lock control unit, and/or the like.

In step S516, the main module controls the server module to send an acknowledgment message to the access control management system indicative of that the lock control unit is installed at the previously specified location. The acknowledgment message causes the access control management system to update its database by associating the lock control unit with the location (step S517). After sending the acknowledgment message the process may e.g. terminate or return to a previous step, e.g. step S508.

22

In the following, example of configuration steps for configuring a lock control unit will be described in more detail.

An "open lock" configuration step may comprise sending an "open door" command to the lock control unit so as to cause the lock control unit to activate the lock mechanism so as to provide access to the location. This step allows the technician to verify that the associated electronic key is received and verified successfully by the lock control unit, and that the lock control unit correctly activates the lock mechanism. Optionally, the "open lock" command may comprise a parameter indicative of a time period for which the lock mechanism should be activated, e.g. a number of seconds.

A "get signal strength" configuration step may comprise sending a corresponding command to the lock control unit that causes the lock control unit to send the current setting of the signal strength of the communications interface of the lock control unit. The signal strength may then be displayed on by the display module of the mobile unit.

The transmission power of the wireless communications device, e.g. Bluetooth device, in the lock control unit may be adjusted in order to correspond to the surroundings and the environment. A higher transmission strength results in a user mobile unit being able to detect the lock control unit and to initiate the key exchange with the lock control unit from a larger distance. On the other hand, if the transmission power is low, a mobile unit may detect the lock control unit and initiate a key exchange only when the mobile unit is in close proximity to the lock control unit. As the detection and key exchange process require some time, a user approaching a locked door may arrive at the door before the key exchange process has been completed and the lock has been activated, thus resulting in unnecessary delays. If the transmission strength is too large, a lock may be activated while the user is still relatively far away from, and even out of sight of, the lock when the lock is activated, thus reducing the security of the system. Hence, the transmission power or signal strength of the lock control unit should preferably be adjusted to account for the local environment. The range may depend on the strength of the Bluetooth unit(s) and/or on the surroundings, such as the thickness and the material which walls and door are made of. The maximal distance, which the Bluetooth devices in a mobile unit and in a door unit typically can communicate over, is in the range of 50 meter. Furthermore, the lock control unit may have a lag time indicative of a time interval between a successful key verification until the lock control unit activates the lock mechanism. Another example of a parameter influencing the timing of the lock activation is the time during which the lock control unit activates the lock. Some or all of the above parameters may thus be adjusted so as to suitably calibrate the timing of the lock activation relative to a normal approach of a user holding a user mobile unit.

Accordingly, a "set signal strength" configuration step may comprise sending a corresponding command to the lock control unit that causes the lock control unit to set the signal strength of the communications interface of the lock control unit to a given value or to adjust the current setting by a given increment. The value or increment is communicated by the mobile unit to the lock control unit as a parameter together with the command. The value or increment may be received from the access control management system or set by the user of the mobile unit.

Similar commands may be provided allowing the mobile unit to set other parameters of the lock control unit or manually activate selected functions of the lock control unit,

23

e.g. a lag time or duration of the unlocking signal. For example, a command may cause the lock control unit to turn an audible or a visual indicator, such as an LED, ON or OFF.

A “get software version” configuration step may comprise sending a corresponding command to the lock control unit that causes the lock control unit to send a version identifier of the currently installed software version of the lock control unit to the mobile unit. The software version may then be displayed on by the display module of the mobile unit. Similar commands may be provided allowing the mobile unit to request and receive other parameters from the lock control unit, such as an identifier identifying a hardware version of the lock control unit, a battery status of the lock control unit, a battery voltage, a status of a relay for controlling the lock mechanism, and/or the like.

Although some embodiments have been described and shown in detail, the invention is not restricted to them, but may also be embodied in other ways within the scope of the subject matter defined in the following claims. In particular, it is to be understood that other embodiments may be utilised and structural and functional modifications may be made without departing from the scope of the present invention.

In device claims enumerating several means, several of these means can be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims or described in different embodiments does not indicate that a combination of these measures cannot be used to advantage.

It should be emphasized that the term “comprises/comprising” when used in this specification is taken to specify the presence of stated features, integers, steps or components but does not preclude the presence or addition of one or more other features, integers, steps, components or groups thereof.

The invention claimed is:

1. A method of configuring a lock control unit of an access control system, the lock control unit being operationally connected to a lock mechanism for securing a location, the lock control unit having associated with it a lock control unit identifier and electronic key verification data, the lock control unit comprising means for wireless communication via a wireless communications channel with a user mobile unit, and adapted to receive a data item indicative of an electronic key from a user mobile unit, to verify a received electronic key based on the electronic key verification data and, subject to successful verification, to activate the lock mechanism, the method comprising performing the following steps by a technician mobile unit:

receiving a message from an access control management system, the message comprising an address indicative of the location;

detecting one or more lock control units communicating via the wireless communications channel in a proximity of the technician mobile unit; and receiving from each detected lock control unit a respective lock control unit identifier;

identifying, based on the received lock control unit identifiers, the lock control unit connected to the lock mechanism;

sending the lock control unit identifier indicative of the lock control unit identified by the technician mobile unit to the access control management system;

receiving, from the access control management system, an electronic key associated with the lock control unit identifier;

24

sending one or more commands to the lock control unit causing the lock control unit to perform one or more configuration steps;

sending a message from the technician mobile unit to the access control management system, the message being indicative of a completion of the configuration steps; wherein the method further comprises associating, by the access control management system and responsive to the message indicative of a completion of the configuration steps, the lock control unit identifier of the lock control unit connected to the lock mechanism with the address of the location.

2. A method according to claim 1, wherein performing at least one of the one or more configuration steps comprises setting one or more configuration parameters of the lock control unit or receiving at least one value of at least one operational parameter from the lock control unit.

3. A method according to claim 2, wherein the predetermined communication channel is a short-range radio-frequency communication channel, wherein the lock control unit comprises a radio transmitter for communicating via the short-range radio-frequency channel; and wherein setting one or more configuration parameters comprises setting a transmission power of the radio transmitter.

4. A method according to claim 1, wherein detecting one or more lock control units communicating via the wireless communications channel in a proximity of the technician mobile unit includes detecting all electronic devices communicating via the wireless communications channel within a communication range of the technician mobile unit, and, for each detected device, determining whether the detected device is a lock control unit.

5. A method according to claim 1, further comprising, displaying a list of configuration steps, receiving a user-selection of one or more of the configuration steps, and, responsive to the received user-selection, sending the one or more commands to the lock control unit causing the lock control unit to perform one or more configuration steps.

6. A method according to claim 1, wherein receiving an electronic key associated with the lock control unit identifier comprises receiving one or more commands indicative of one or more configuration steps to be performed.

7. A method according to claim 1, wherein sending one or more commands to the lock control unit comprises sending a data item indicative of the received electronic key so as to cause the lock control unit to verify the electronic key.

8. A method according to claim 1, further comprising authenticating the technician mobile unit and/or a user of the technician mobile unit by the access control management system.

9. A method of controlling access to a location, the method comprising configuring a lock control unit of an access control system by performing the steps of the method defined in claim 1, and performing the following steps by a user mobile unit:

receiving an electronic key from the access control management system, the electronic key being indicative of a predetermined access right to the location, the electronic key having associated with it a lock control unit identifier of a lock control unit associated with the location;

detecting one or more lock control units communicating via the wireless communications channel in a proximity of the user mobile unit;

identifying, based on the lock control unit identifier, the lock control unit associated with the location; and

25

sending a data item indicative of the electronic key to the lock control unit causing the lock control unit to authenticate the electronic key and, subject to successful authentication of the electronic key, to operate a lock mechanism.

10. An access control system comprising an access control management system, a technician mobile unit and a lock control unit; wherein the access control system is configured to perform the steps of the method defined in claim 1.

11. A method according to claim 2, wherein detecting one or more lock control units communicating via the wireless communications channel in a proximity of the technician mobile unit includes detecting all electronic devices communicating via the wireless communications channel within a communication range of the technician mobile unit, and, for each detected device, determining whether the detected device is a lock control unit.

12. A method according to claim 2, further comprising, displaying a list of configuration steps, receiving a user-selection of one or more of the configuration steps, and, responsive to the received user-selection, sending the one or more commands to the lock control unit causing the lock control unit to perform one or more configuration steps.

13. A method according to claim 2, wherein receiving an electronic key associated with the lock control unit identifier comprises receiving one or more commands indicative of one or more configuration steps to be performed.

14. A method according to claim 2, wherein sending one or more commands to the lock control unit comprises sending a data item indicative of the received electronic key so as to cause the lock control unit to verify the electronic key.

15. A method according to claim 2, further comprising authenticating the technician mobile unit and/or a user of the technician mobile unit by the access control management system.

16. A method according to claim 9, wherein the configuring a lock control unit of an access control system is carried out by the steps of the method defined in claim 2.

26

17. A method according to claim 9, wherein the configuring a lock control unit of an access control system is carried out by the steps of the method defined in claim 3.

18. An access control management system for controlling access to a plurality of locations, each location being secured by a respective lock mechanism, each lock mechanism being controlled by a lock control unit, the lock control unit having associated with it a lock control unit identifier and electronic key verification data, the lock control unit comprising means for wireless communication via a wireless communications channel with a user mobile unit, and adapted to receive a data item indicative of an electronic key from a user mobile unit, to verify a received electronic key based on the electronic key verification data and, subject to successful verification, to activate the lock mechanism, the access control management system being configured to perform the following steps:

sending a message to a technician mobile unit, the technician mobile unit comprising means for wireless communication via the wireless communications channel with the lock control unit, the message comprising an address indicative of the location;

receiving from the technician mobile unit, a lock control unit identifier indicative of a lock control unit identified by the technician mobile unit to be connected to a lock mechanism of the location;

sending to the technician mobile unit an electronic key associated with the lock control unit identifier, causing the technician mobile unit to send one or more commands to the lock control unit causing the lock control unit to perform one or more configuration steps;

receiving a message from the technician mobile unit, the message being indicative of a completion of the configuration steps; and

associating, responsive to the received message, the lock control unit identifier of the lock control unit connected to the lock mechanism with the address of the location.

* * * * *